

Administración de Servicios de Infraestructura IT a través de Zentyal Server 6.2

Cristhian David Arango Ruiz
e-mail: integrante1@institución (quitar hipervínculo)
Leonardo Castiblanco Torres
e-mail: integrante2@institución (quitar hipervínculo)
Jennifer Andrea Fajardo Bolívar
e-mail: jafajardob@unadvirtual.edu.co
Daniel Alfonso Mateus
e-mail: damateusr@unadvirtual.edu.co
Juan Carlos Rodríguez Suarez
e-mail: jcrodriguezsu@unadvirtual.edu.co

RESUMEN: Se realiza la instalación y configuración de la distribución GNU/Linux basada en Ubuntu, Zentyal Server 6.2 para el control y la administración de diferentes servicios de infraestructura IT. Se establece Zentyal como sistema operativo base para poner en marcha los diferentes servicios, como intermediario Endian FireWall, esto con el fin de proteger la red de amenazas externas y las estaciones de trabajo GNU/Linux Ubuntu 18.04. A partir del establecimiento de dicha arquitectura se implementaron los servicios de configuración de red (DHCP), Resolución de nombres de dominio DNS, Controlador de Dominio, Proxy HTTP, Cortafuegos, Carpetas compartidas e impresoras y Redes Virtuales Privadas VPN.

ABSTRACT: The installation and configuration of the GNU / Linux distribution based on Ubuntu, Zentyal Server 6.2 is carried out for the control and administration of different IT infrastructure services. Zentyal is established as the base operating system to start the different services, as an Endian FireWall intermediary to protect the network from external threats, and as a GNU / Linux Ubuntu 18.04 workstation. From the establishment of this architecture, the network configuration services (DHCP), DNS domain name resolution, Domain Controller, HTTP Proxy, Firewall, Shared folders and printers, VPN Virtual Private Networks were implemented.

PALABRAS CLAVE: cliente, cortafuegos, debian, dominio, DMZ, interfaces, IP, IT, panel, proxy, red, servicios, servidor, Ubuntu, usuario, VPN, Zentyal.

I. INTRODUCCIÓN

Este artículo incluye la descripción de la instalación y configuración de Zentyal Server 6.2, donde se implementan los servicios de infraestructura IT para permitir el acceso de una estación de trabajo GNU/Linux Ubuntu 18.04 mediante autenticación con usuario y contraseña y mantener sus registros a través de un controlador de dominio; control de la conectividad a Internet desde Zentyal mediante un Proxy; establecimiento de restricciones de apertura de redes

sociales o sitios web de entretenimiento; acceso a carpetas compartidas e impresoras y la creación de una VPN que permita la comunicación con la estación de trabajo a través de un túnel privado de comunicación.

A. Instalación de Zentyal

1. Se realiza la instalación de Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT, para ello Server se debe disponer del disco de arranque o pendrive booteable con este sistema, para este ejercicio se descargará desde el sitio oficial <https://zentyal.com/es/inicio/>.



Figura 1. Confirmación de Instalación Zentyal 6.2.

Esta distribución se obtendrá por 45 días de manera gratuita, para ello se debe seleccionar el icono naranja, el cual redireccionará a una nueva página, allí se deben ingresar datos y así obtener una licencia de activación.

2. Una vez se tiene al archivo .iso se crea una nueva máquina virtual.

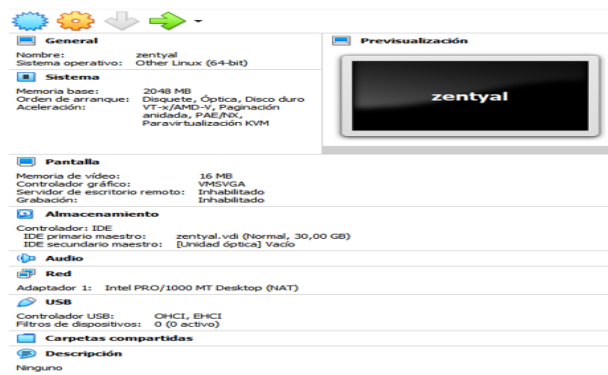


Figura 2. Información detallada de nueva máquina virtual.

- Una vez realizadas esta configuración se inicia la instalación de Zentyal, para lo cual se debe primero elegir el idioma de preferencia.

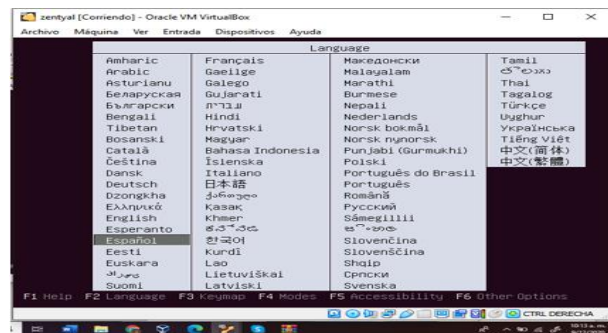


Figura 3. Selección de idioma.

- El asistente muestra un menú de arranque, para lo cual se selecciona el modo requerido, para este caso se elige la primera opción *instalar Zentyal comercial (borrar todo el disco)*, dado a que es la primera instalación que se está realizando.

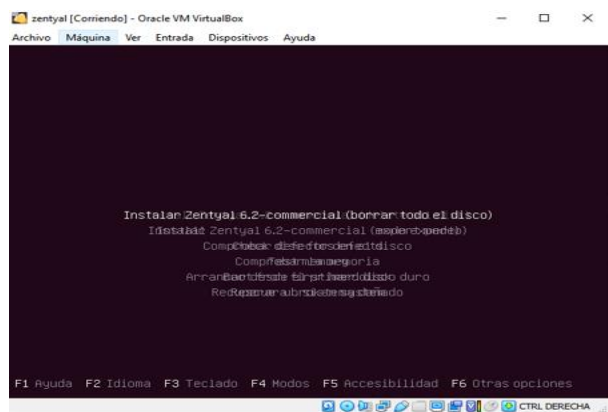


Figura 4. Instalación Zentyal.

- Durante el proceso de instalación se solicitan realizar diferentes configuraciones dentro de las cuales están ubicación para fijar la zona horaria y teclado.

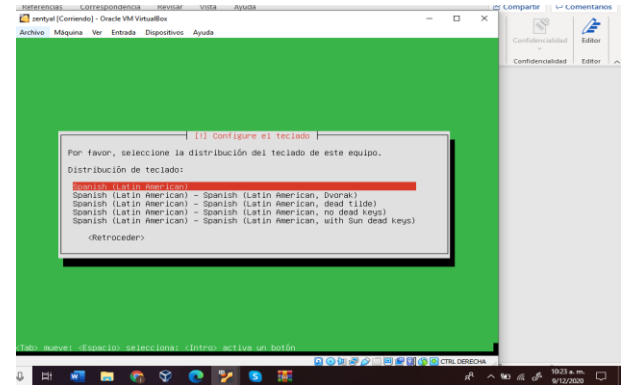


Figura 5. Configuración de teclado en Zentyal.

- En una nueva ventana el asistente solicitará al administrador la configuración de red para esta máquina, para ello se debe indicar el nombre de esta, es así como se podrá encontrar en la red.

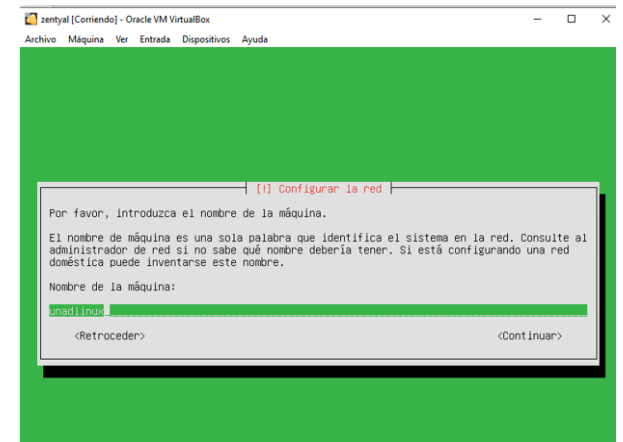


Figura 6. Configuración de red en Zentyal.

- Posteriormente se confirma la configuración del reloj utilizando la zona horaria America/Bogota, para esto se debe dar Enter en la opción SI, si está correcto. Una vez configurado el reloj empieza la instalación del sistema.

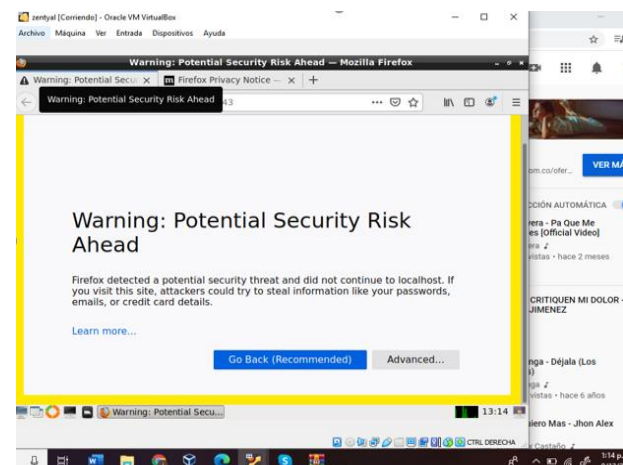


Figura 7. Primera interfaz de inicio en Zentyal.

B. DHCP Server, DNS Server y Controlador de Dominio

Para poder iniciar con la configuración se debe como mínimo realizar la instalación de forma típica, configurando al menos un adaptador de red y conectarlo a la red interna DMZ con Endian, posteriormente, se procede con la instalación habitual hasta acceder al panel de administración de Zentyal.

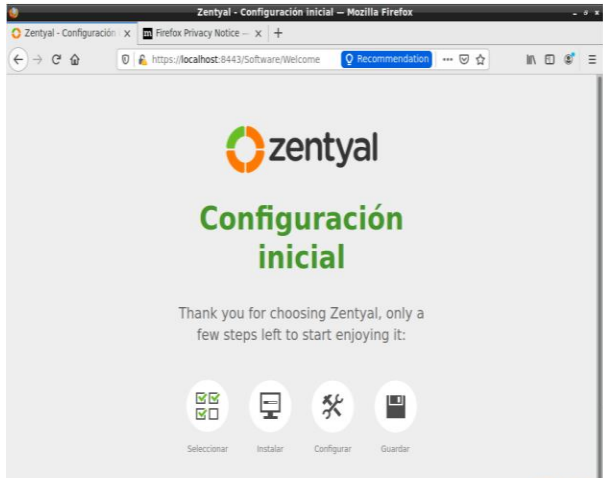


Figura 8. Confirmación de Instalación Zentyal 6.2.

Los pasos requeridos para esto son:

1. Instalación paquetes: Para proceder con la configuración inicial se instalan los paquetes necesarios para poder establecer el controlador de dominio requerido.

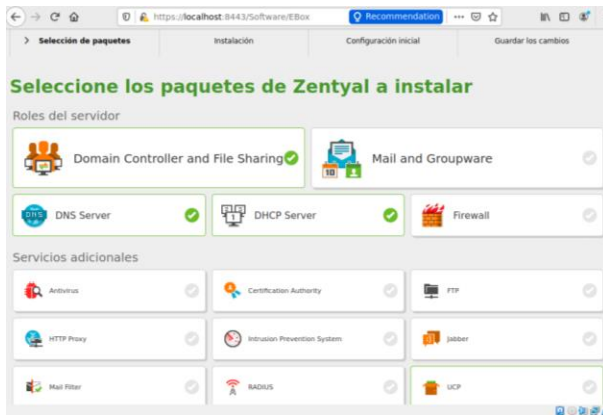


Figura 9. Instalación Paquetes necesarios.

2. Configuración Inicial: Se Define las interfaces de red necesarias, la tarjeta eth0 se configurará externa que, para garantizar la conexión a internet, la tarjeta eth1, será interna y se le asignará una dirección IP estática, en el rango de direcciones del DMZ. Así como el nombre de dominio que será clave para lograr el objetivo.



Figura 10. Configuración de Interfaces de Red.



Figura 11. Definición del nombre de dominio.

3. Configuración Ficheros resolv.conf y hosts: Para agregar el DNS definido en la configuración de y el host y la dirección ip de Zentyal.

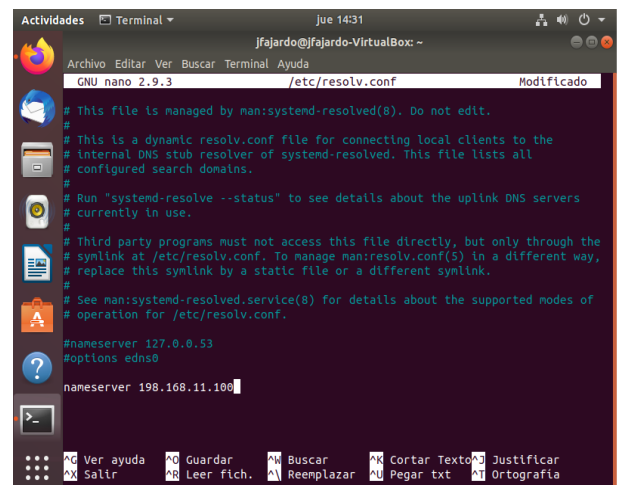


Figura 12. Configuración resolv.conf.

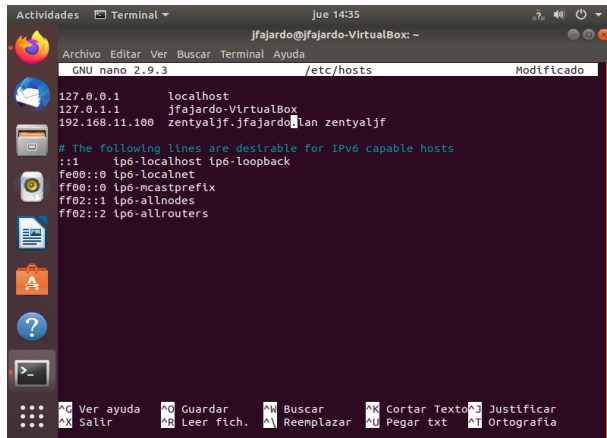


Figura 13. Configuración hosts.

4. Añadir usuario Zentyal para acceso de la estación de trabajo: Se define el usuario, contraseña y grupo del usuario con el que se permitirá el acceso a la estación de trabajo GNU/Linux.



Figura 14. Creación usuario en Zentyal.

5. Instalación PBIS-open: Se procede con la instalación en la estación de trabajo GNU/Linux Ubuntu de la aplicación PBIS-open para unirla al dominio.

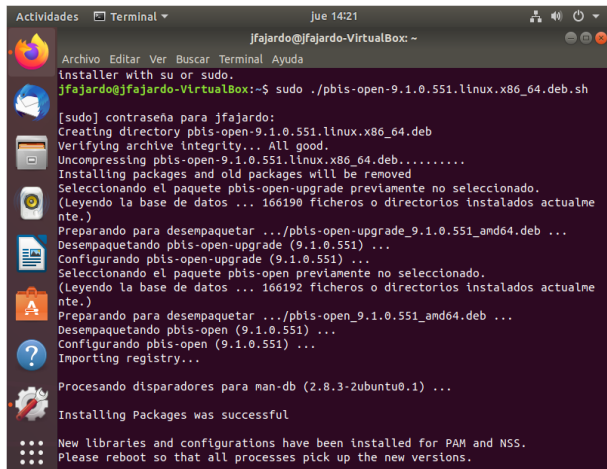


Figura 15. Instalación PBIS-open en Desktop.

6. Se une la máquina al dominio:

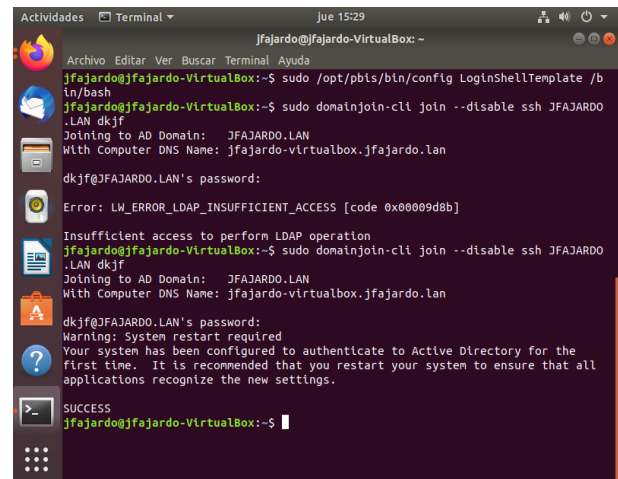


Figura 16. Uniendo la máquina al dominio.

7. Se accede desde la estación GNU/Linux: Con las credenciales definidas en Zentyal y al acceder en la configuración del usuario se puede observar los datos que se asignaron en la creación del usuario dkjf, Jennifer Fajardo.



Figura 17. Ingresando a la estación de trabajo.

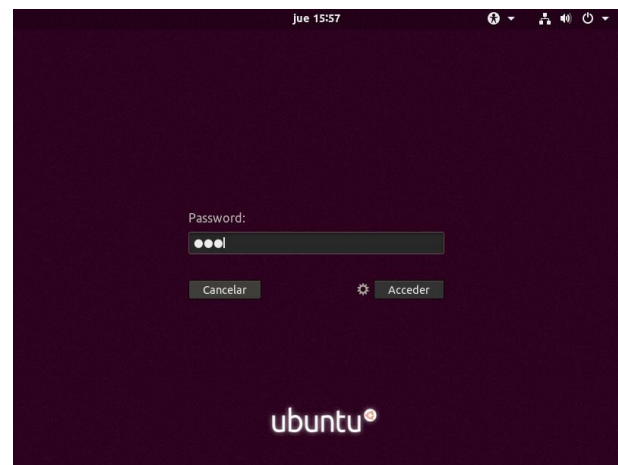


Figura 18. Ingresar contraseña de usuario.

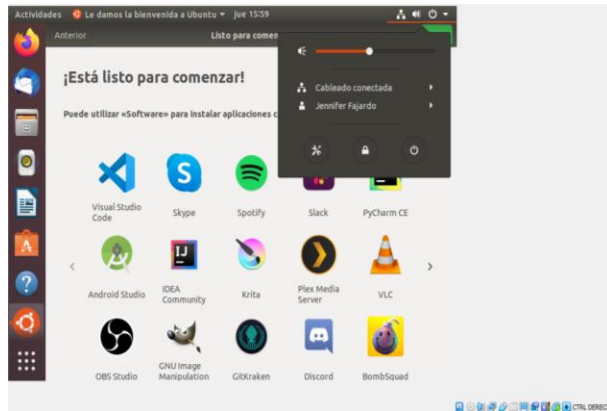


Figura 19. Comprobar acceso a la estación de trabajo.

- Verificación de que el equipo está en conexión a través de Usuarios y equipos y la opción Computers donde se ve la estación GNU/Linux vinculada.

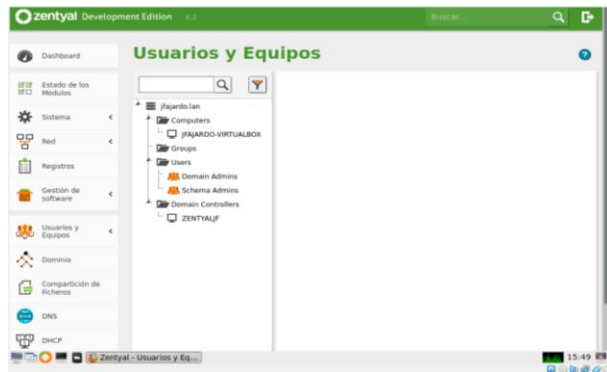


Figura 20. Estación GNU/Linux agregada.

C. Proxy no Transparente

Para la implementación del proxy no transparente en Zentyal, es necesario la instalación y configuración del módulo HTTP Proxy en nuestro servidor Zentyal, una vez instalado procedemos a realizar los siguientes cambios:

- Se valida que la opción proxy transparente se encuentre deshabilitada.

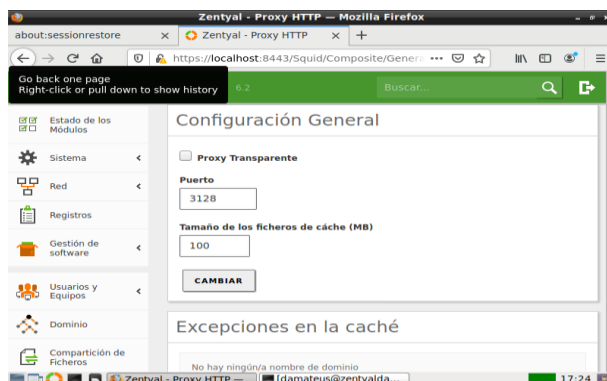


Figura 21. Proxy transparente deshabilitado.

- Se procede a crear el perfil de filtrado, sobre el cual relacionaremos los sitios web a los cuales permitiremos o denegaremos el acceso.

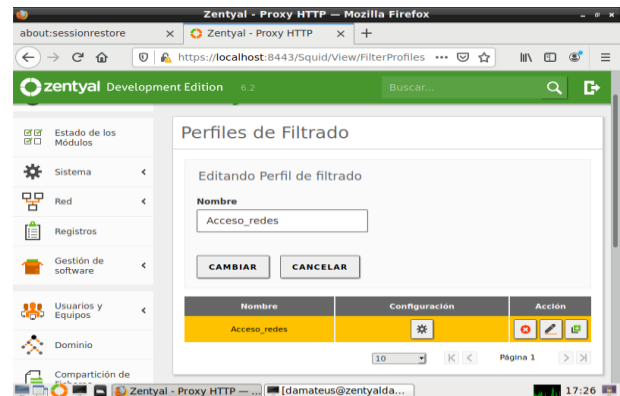


Figura 22. Perfiles de filtrado.

- Una vez creado el perfil de acceso se crean las reglas de acceso asociadas al perfil previamente creado, para ello hacemos uso de la opción Reglas de acceso.

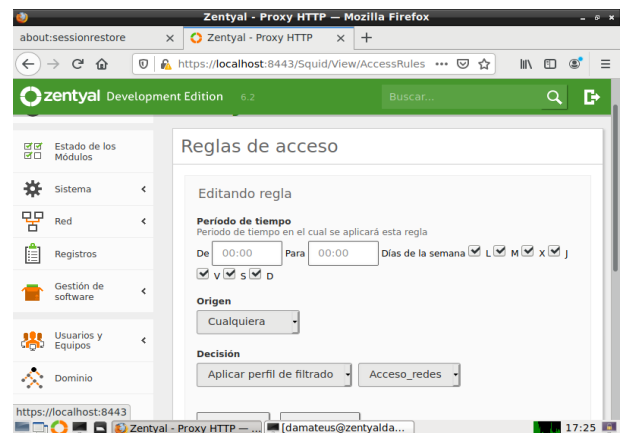


Figura 23. Reglas de acceso.

- Ahora hacemos uso de la opción Perfiles de Filtrado en donde se nos visualiza el perfil que hemos creado previamente, pulsamos el botón Configurar.

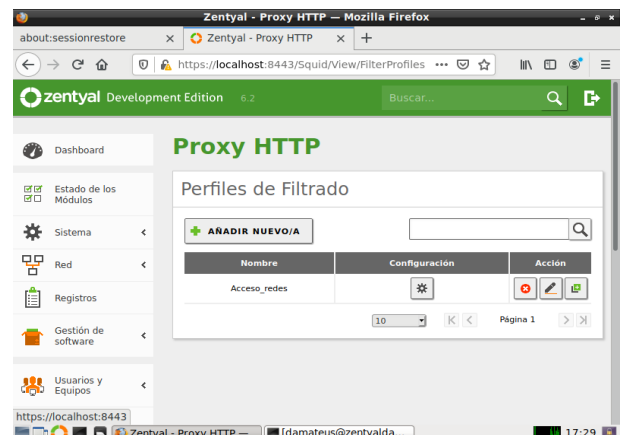


Figura 24. Editar perfil de filtrado.

5. Seguidamente seleccionamos el Umbral, el cual aplicara sobre el perfil, en este caso seleccionaremos Estricto.

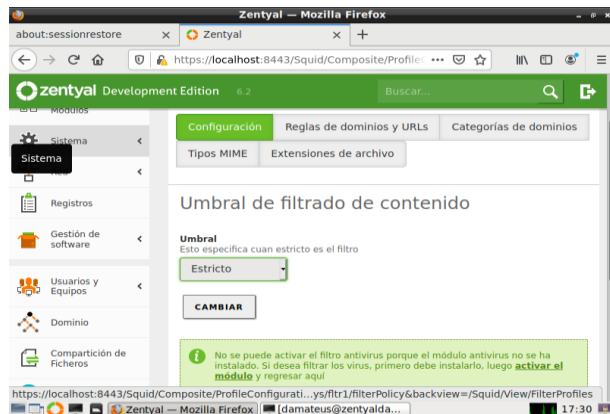


Figura 25. Umbral de filtrado.

6. Seleccionamos la pestaña Reglas de dominios y URL's, allí ingresamos los dominios sobre los cuales permitiremos o denegaremos el acceso.

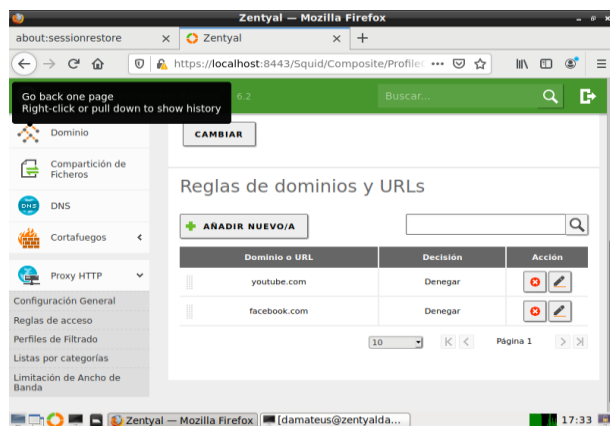


Figura 26. Reglas de dominio.

7. En nuestra maquina virtual cliente debemos configurar la red, de manera que quede asignada a la misma red del servidor Zentyal, en este caso la ip del Zentyal es: 192.168.1.2, así que nuestro cliente debe estar en la misma red, por ende se asigna la ip 192.168.1.3 y como Gateway la ip 192.168.1.1.

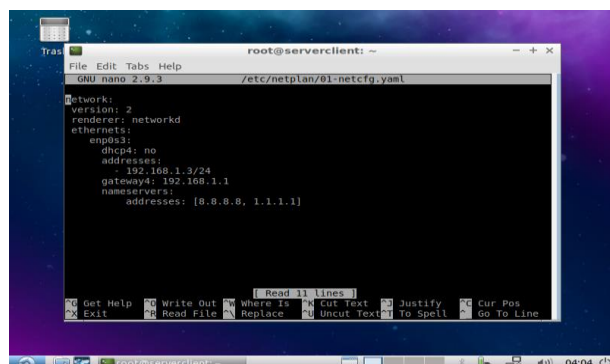


Figura 27. Configurar ip en el cliente.

8. Se valida que las maquinas virtuales se encuentren en la misma red y puedan visualizarse, a su vez que ambas tengan acceso a internet.



Figura 28. Acceso a internet en el cliente.

9. Una vez se confirma que hay conexión entre las maquinas y que hay internet, se procede a configurar el proxy Zentyal en nuestra maquina cliente.

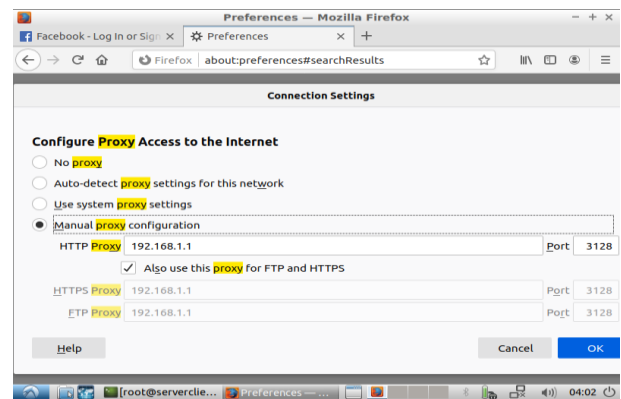


Figura 29. Configuración proxy en el cliente.

10. Una vez se han guardado y aplicado los cambios, procedemos a realizar la prueba, ingresando a uno de los dominios a los cuales denegamos el acceso, por ejemplo facebook.com.

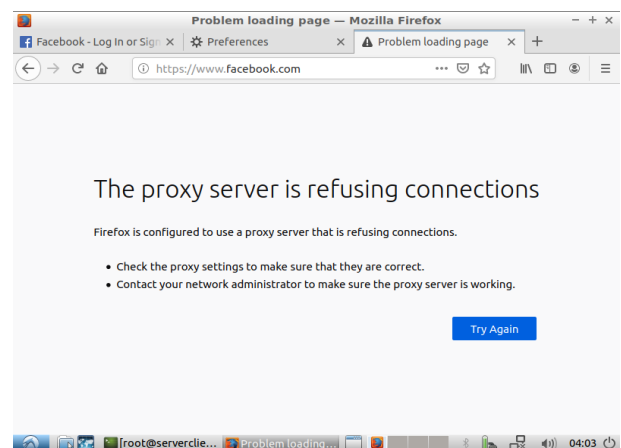


Figura 30. Sitio restringido por proxy.

D. Cortafuegos

Dentro de las interfaces de red se establecerá la red externa WAN y la red interna LAN, siendo la última configurada bajo el método estático, por lo cual se le otorgará una IP fija.

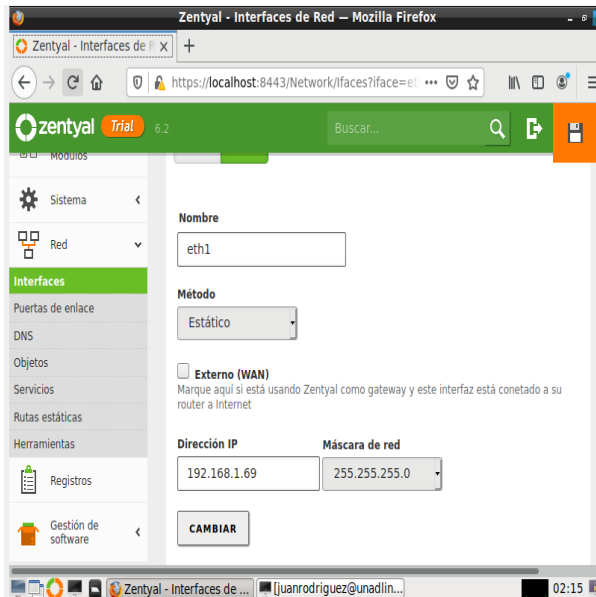


Figura 31. Configuración interfaces de red.

Si se desea realizar la restricción a un pool específico de IPs se debe primero configurar en Zentyal el servicio DHCP para que las máquinas conectadas a la red tomen la IP de dicho rango.

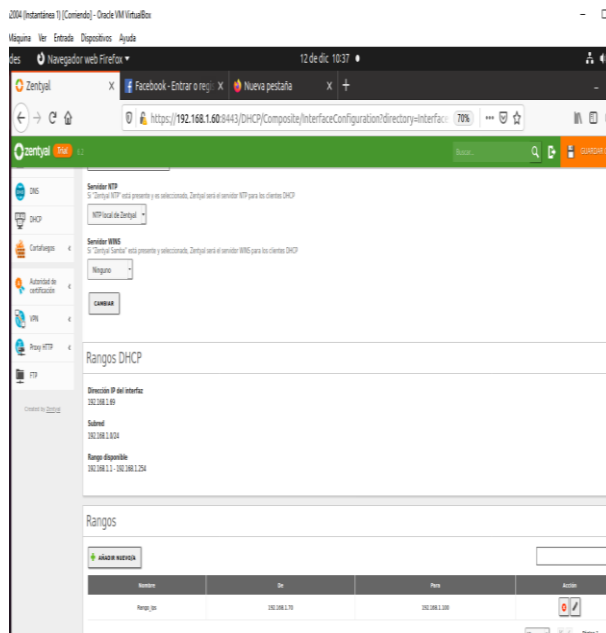


Figura 32. Configuración rangos DHCP para red.

Al reiniciar uno de los equipos tomó una de las IPs definidas en dicho rango.

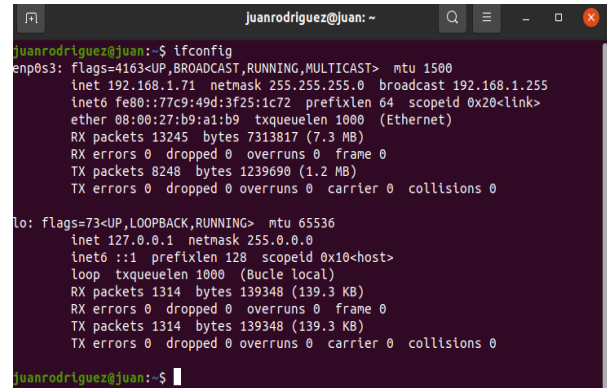


Figura 33. En comando Ifconfig se evidencia que la IP está dentro del rango configurado.

Para poder restringir el acceso a sitios o portales web como Facebook se deberá primero conocer la IP a donde va dirigido, para ello se hará un ping a Facebook desde la máquina GNU/Linux desktop.

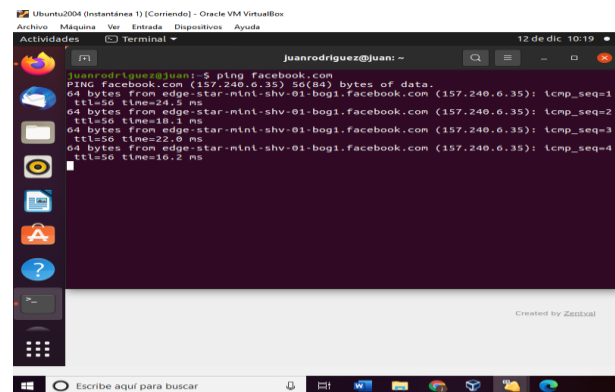


Figura 34. Ping a página Facebook.

Como se puede evidenciar en la imagen anterior la IP destino es 157.240.6.35.

Se procede a realizar la respectiva consulta directamente a Facebook con el fin garantizar que previo a cualquier proceso esté funcionando sin error de conexión alguno.

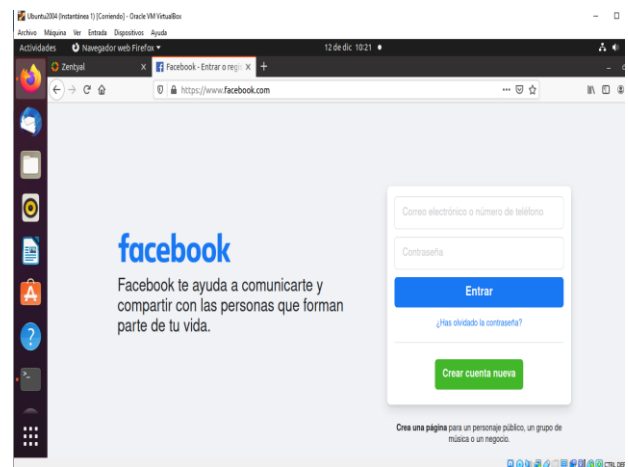


Figura 35. Acceso Enlace a Facebook.

Se deberá incluir el rango de IPs que no podrán ingresar a Facebook, para ello se deberá crear un objeto desde el módulo de red en Zentyal, allí se indica el rango de Ips que no tendrán dicho acceso.

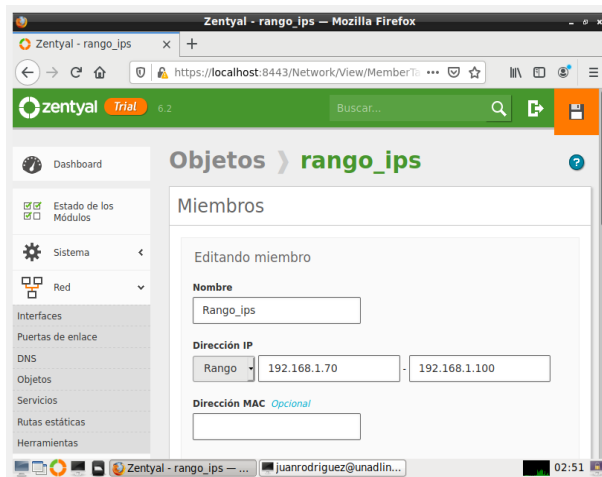


Figura 36. Inclusión de objeto rango Ips.

Posteriormente se deberá establecer el filtrado de paquetes desde la opción Cortafuegos e ingresar a reglas de filtrado para las redes internas.

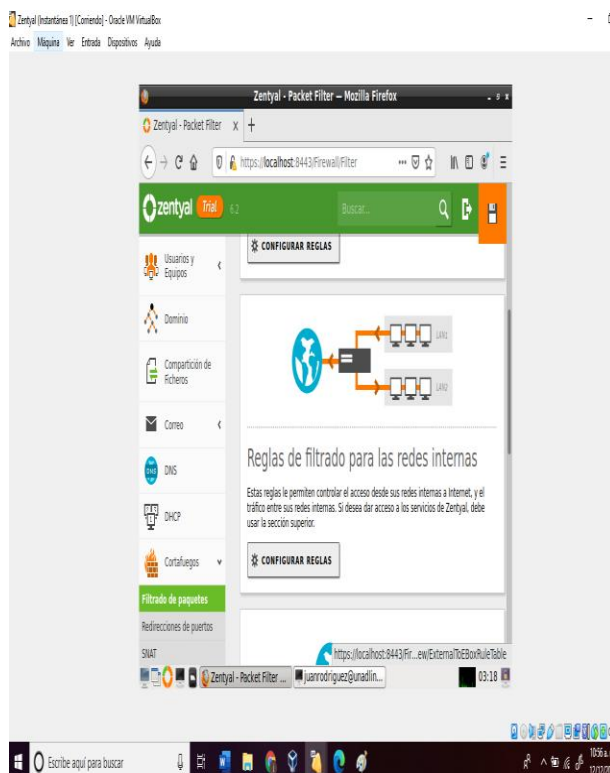


Figura 37. Reglas de filtrado para redes internas.

Al añadir una nueva regla para la restricción se deberá tener en cuenta la IP destino (Facebook) detectada previamente (ver figura 34).

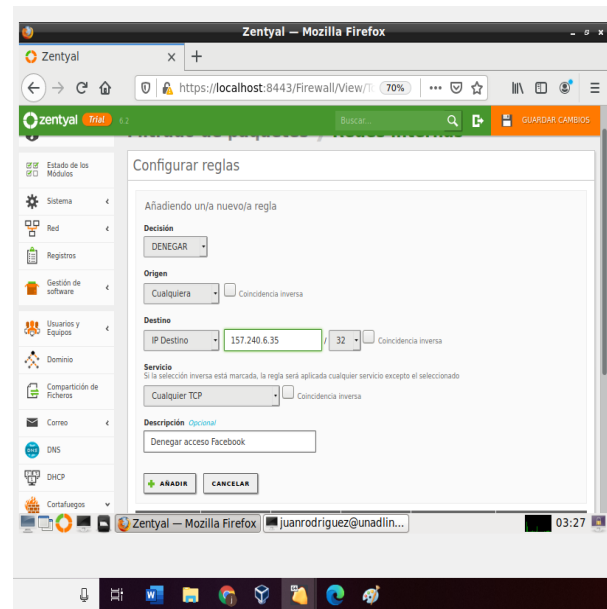


Figura 38. Inclusión de regla para denegar acceso a Facebook por defecto se toma TCP.

Se podrá ahora clonar esta regla para que no permita protocolos HTTP ni HTTPS.

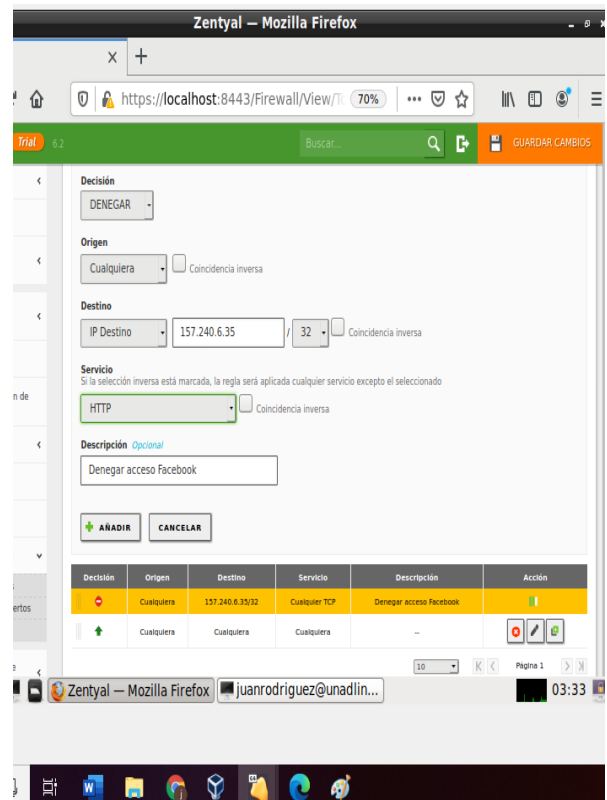


Figura 39. Incluir reglas de filtrado en Zentyal protocolos http y https.

Se podrán consultar como quedan estas reglas una vez configuradas desde Zentyal.

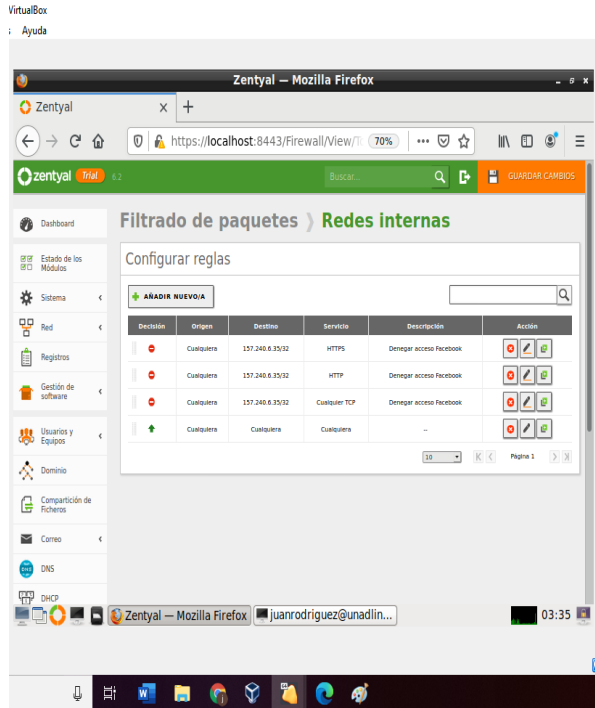


Figura 40, Reglas de filtrado configuradas en Zentyal.

Se procede a consultar desde la maquina GNU/Linux Desktop el sitio restringido en Zentyal.

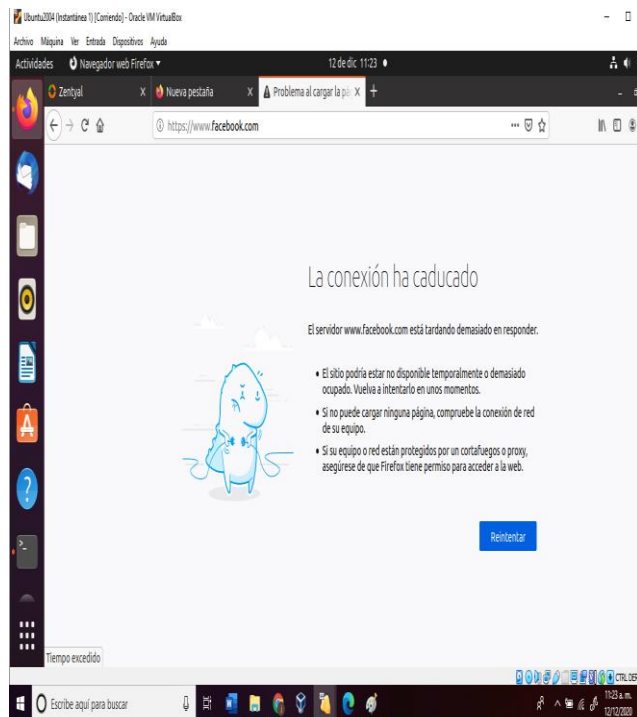


Figura 41. consulta acceso desde la máquina GNU/Linux Desktop.

Por último, se procede a restringir el acceso a otros sitios de entretenimiento.

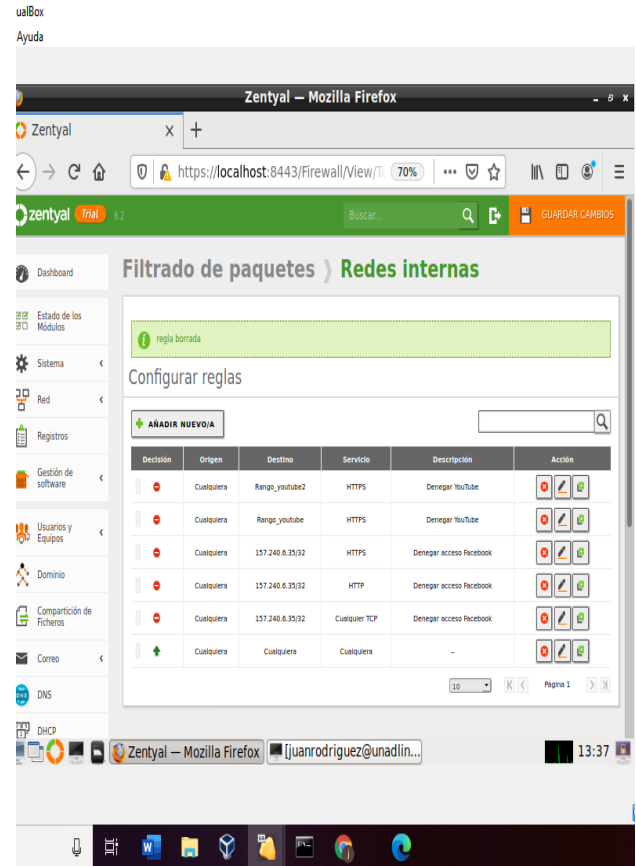


Figura 42. Restricción acceso otros sitios.

E. File Server y Print Server

Antes de esta configuración hemos realizado la instalación de Zentyal Server 6.2 y la configuración del DHCP, ahora vamos al apartado de dominio y vamos a realizar la configuración del mismo. Habilitamos los perfiles móviles además de confirmar el nombre de dominio y netbios de nuestro Server.

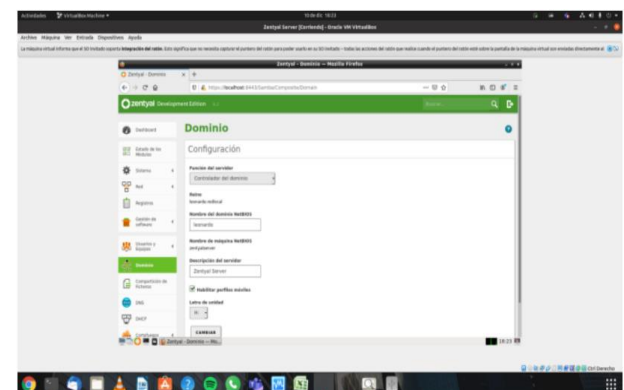


Figura 43. Configuración Dominio.

Ahora, vamos al apartado de usuarios y equipo dentro de zentyal y vamos a configurar un grupo de usuarios llamado familia y dentro 2 nuevos usuarios con los

cuales probaremos que nuestro servidor este configurado correctamente.

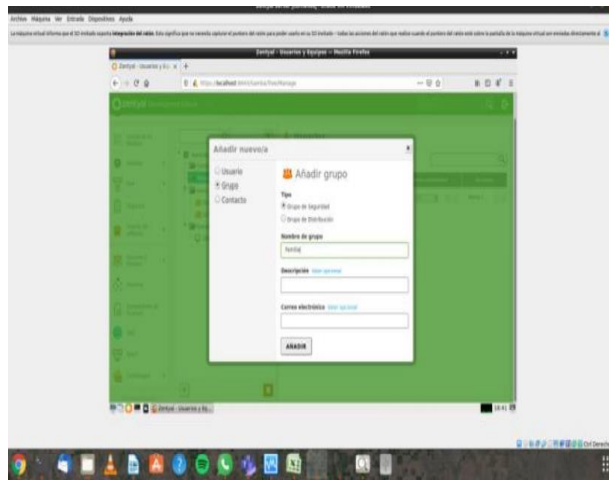


Figura 44. Configuración de grupo de usuarios.

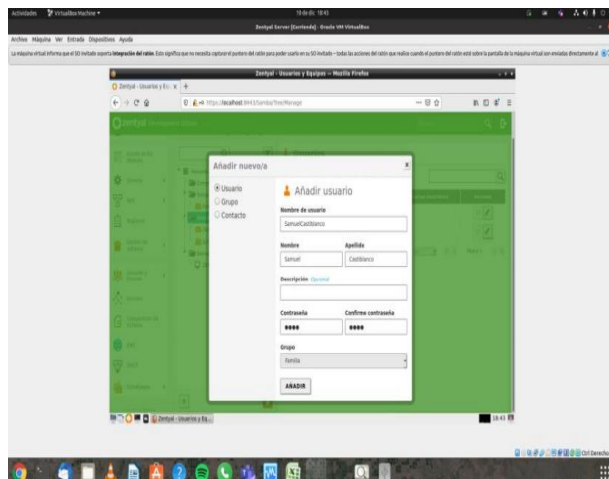


Figura 45. Creación de usuarios dentro del grupo.

A continuación, podemos observar cómo quedó configurado nuestro servidor Zentyal.



Figura 46. Configuración final del grupo.

Hasta este punto hemos configurado nuestro servidor LDAP. Para comprobar su funcionamiento, vamos a iniciar sesión con otra máquina virtual y agregarla al

dominio. Es importante que esta máquina sea configurada con una interfaz de red en modo puente para que quede en comunicación con nuestro servidor.

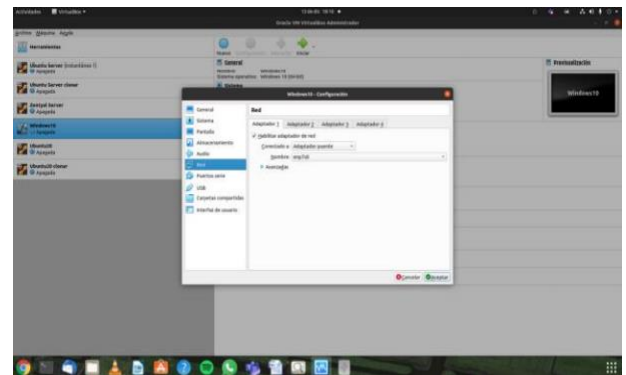


Figura 47. Validación de credenciales en otra máquina virtual.

Iniciamos nuestra maquina normalmente, nos vamos a sistema y damos clic sobre cambiar la configuración del grupo de trabajo. Seleccionamos dominio y escribimos el de nuestro servidor.

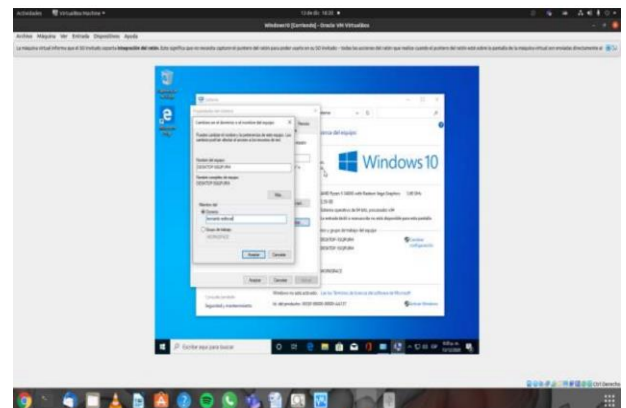


Figura 48. Relación de maquina con el dominio creado.

El sistema nos pedirá las credenciales de autenticación de nuestro servidor. Una vez las ingresamos tendremos nuestro cliente LDAP configurado y podremos iniciar sesión con los usuarios que creamos dentro de Zentyal.

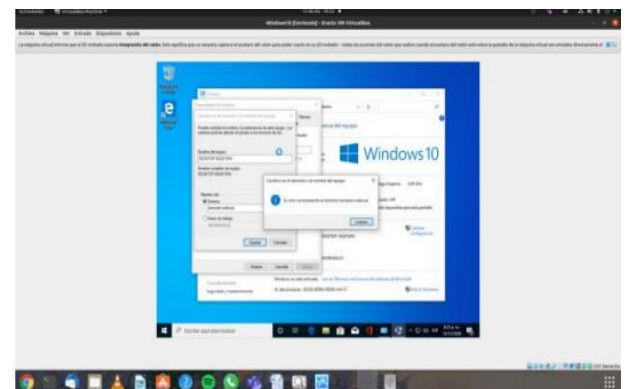


Figura 49. Configuración terminada.

Reiniciamos el cliente e ingresamos con algún usuario de nuestro servidor.

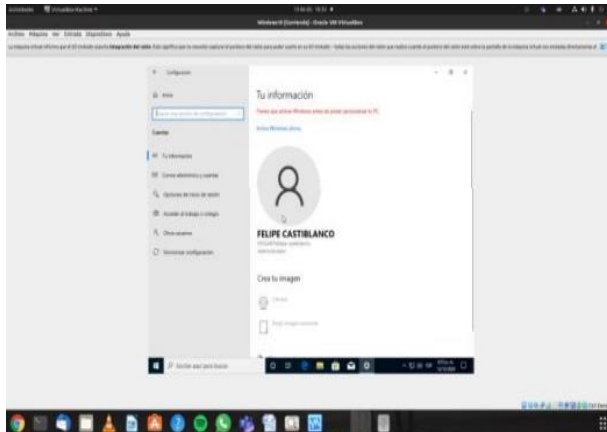


Figura 50. Reiniciar credenciales cliente.

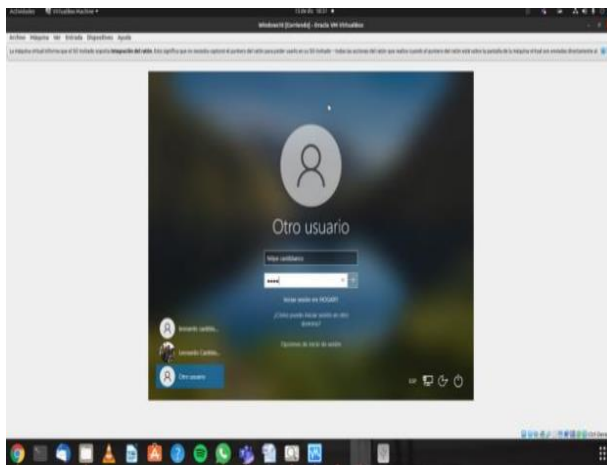


Figura 51. Iniciar sesión con usuario creado en el servidor.

Ya con nuestro servidor LDAP funcionando. Volvemos a Zentyal y configuraremos una carpeta compartida entre mis equipos de la red.

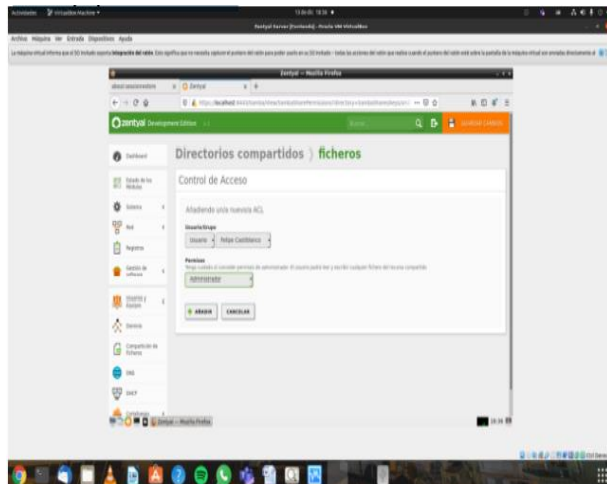


Figura 52. Creación recurso compartido.

Ahora, definimos la ruta y nombre que daremos a nuestra carpeta compartida en la red.

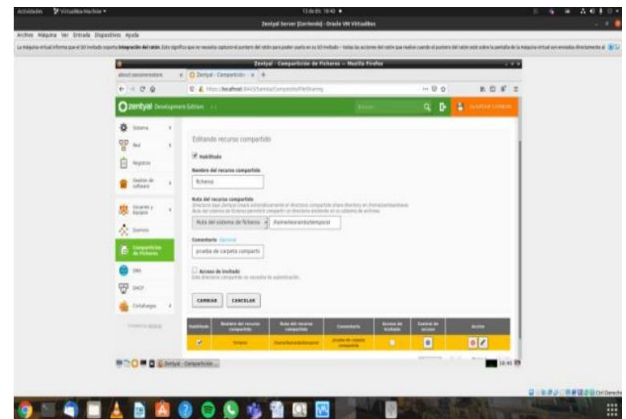


Figura 53. Definición ruta de recurso compartido.

Con el comando MKDIR creamos la carpeta temporal dentro del dentro de la ruta configurada en zentyal. Para finalizar, vamos a nuestro equipo cliente e ingresamos a nuestras rutas compartidas de red.

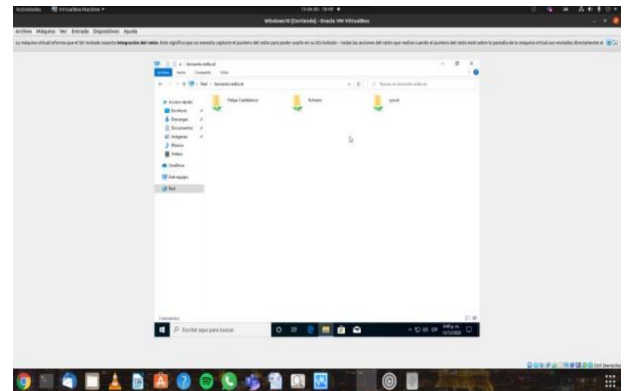


Figura 54. Creación de carpeta temporal.

Ingresamos las credenciales de alguno de los usuarios que tenga permisos a nuestra carpeta compartida.

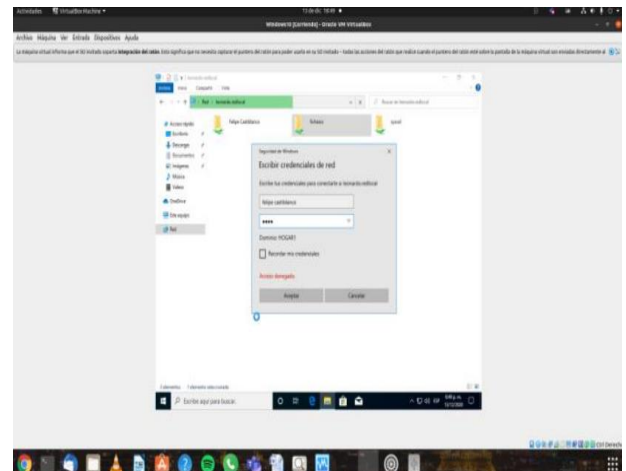


Figura 55. Validación con usuario.

Por último, vamos a crear una carpeta para comprobar los permisos de escritura sobre la ruta.

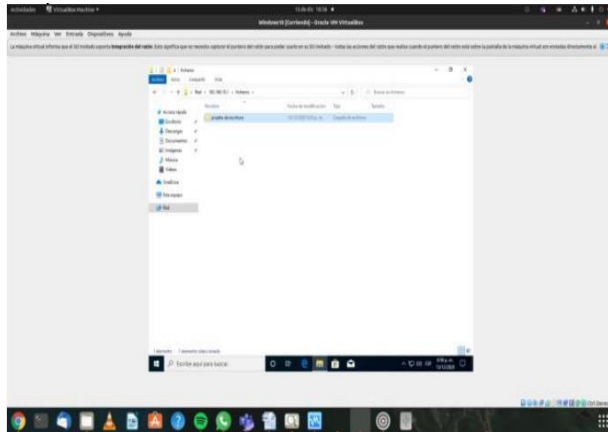


Figura 56. Validación de permisos en ruta.

Ahora, vamos a ingresar a este mismo recurso desde otra máquina virtual que tengamos con Ubuntu Desktop. Es importante mencionar que este también debe estar configurada en modo puente para que nuestro servidor pueda reconocerla desde la red.

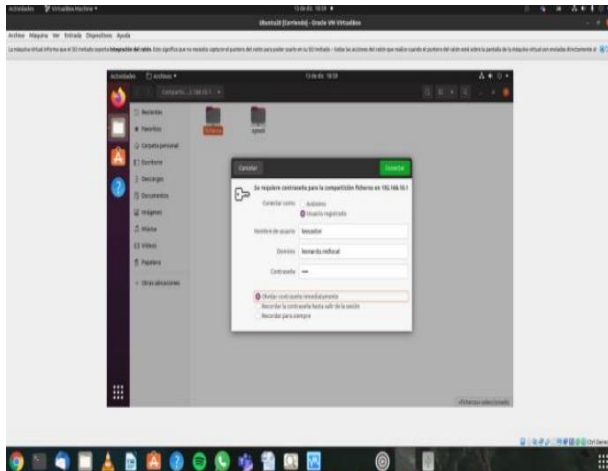


Figura 57. Configuración File server Ubuntu.

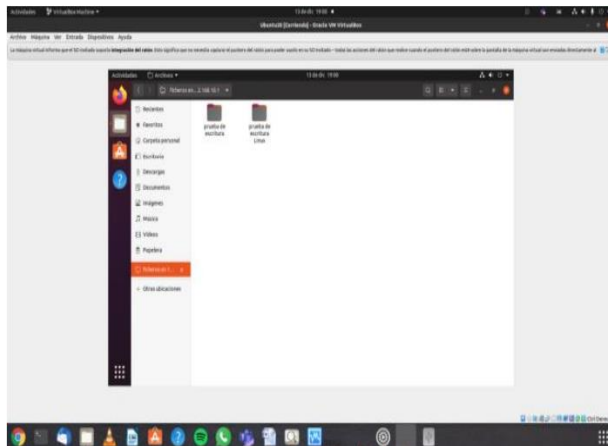


Figura 58. Verificación de acceso, File Server.

F. VPN

Se selecciona Y se instala los siguientes paquetes: Network Configuration, Firewall, Certification Authority y VPN.

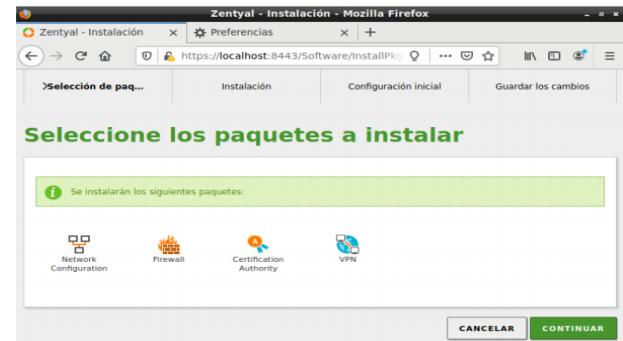


Figura 59. Instalación VPN.

Se configura la red eth0 externa con método DHCP y la eth1 interna con IP estática.

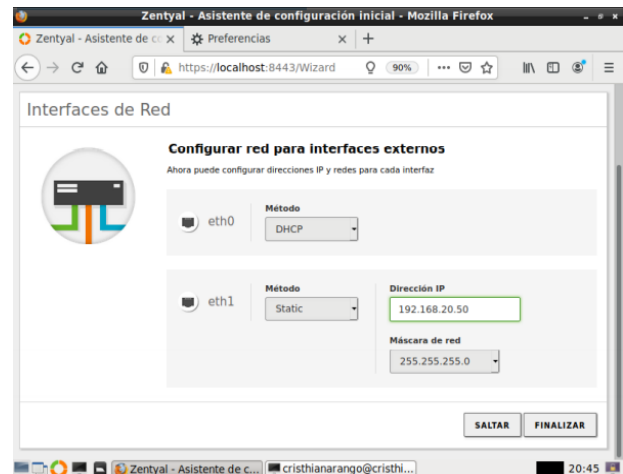


Figura 60. Configuración para interfaces externos.

Creación del certificado de autoridad para zentyal, También se necesita un certificado para el servidor VPN.

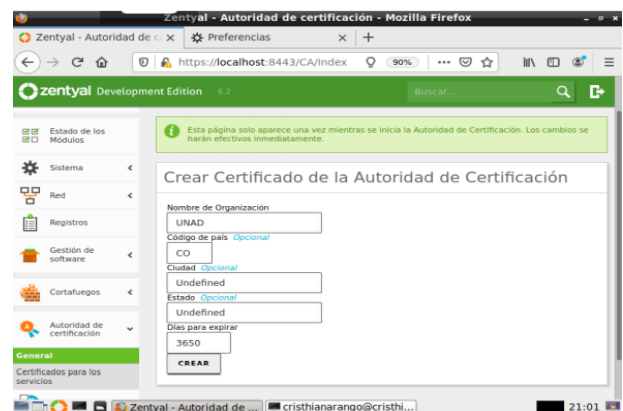


Figura 61. Creación De certificados de autoridad.

Se crea un servidor VPN.

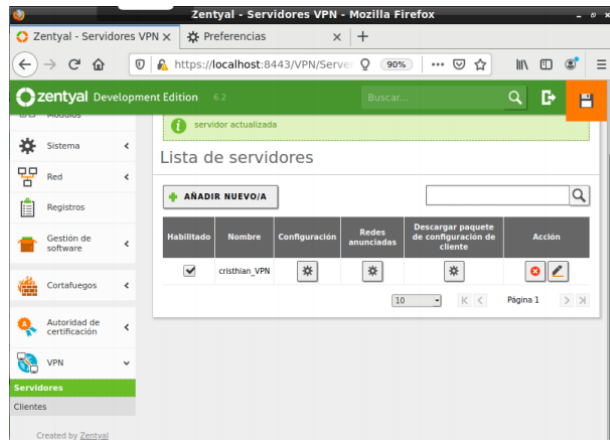


Figura 62. Creación de servidor VPN.

El programa automáticamente realiza toda la configuración lo único que se ingresa es el nombre.

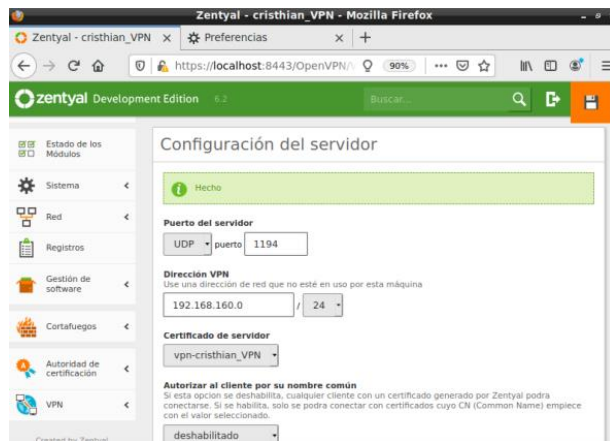


Figura 63. Configuración del servidor.

Creación del certificado para el cliente.

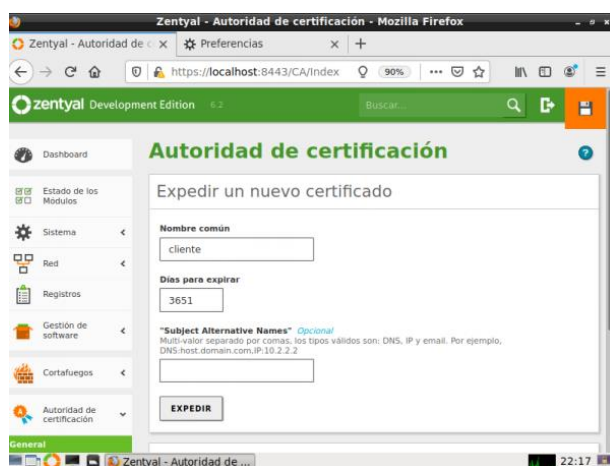


Figura 64. Creación del certificado cliente.

Configuración del servidor VPN para la conexión cliente.

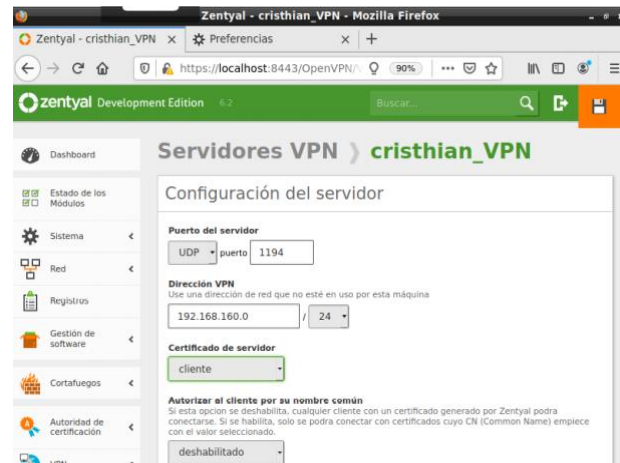


Figura 65. Configuración del servidor VPN cliente.

Configuración de servicios de red que permitirán la conexión del servidor VPN y Configuración del cortafuegos para agregar como regla el servicio.

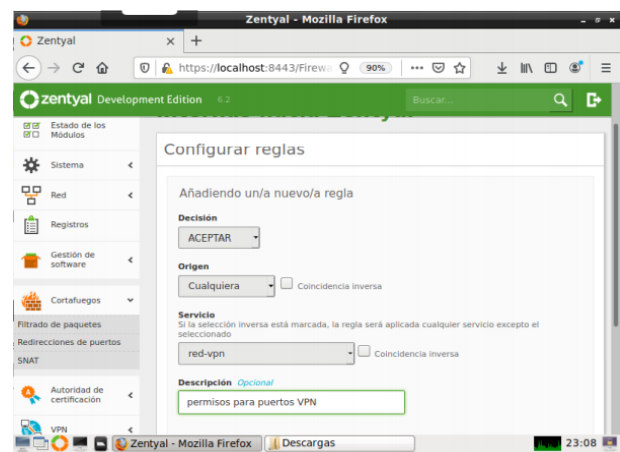


Figura 66. Configuración de servicios de red.

Se descarga el paquete para la instalación en la máquina virtual Ubuntu de escritorio.

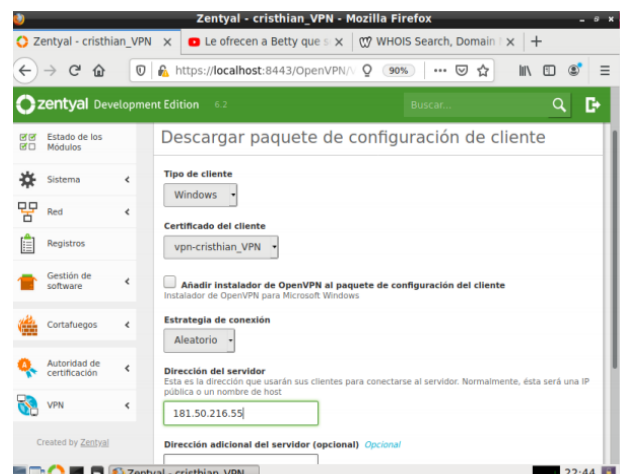


Figura 67. Descarga del paquete VPN cliente.

Ingresamos siguiente ruta y se le quitan las comillas"" a las tres líneas en el recuadro rojo, para la configuración del cliente VPN a Zentyal.

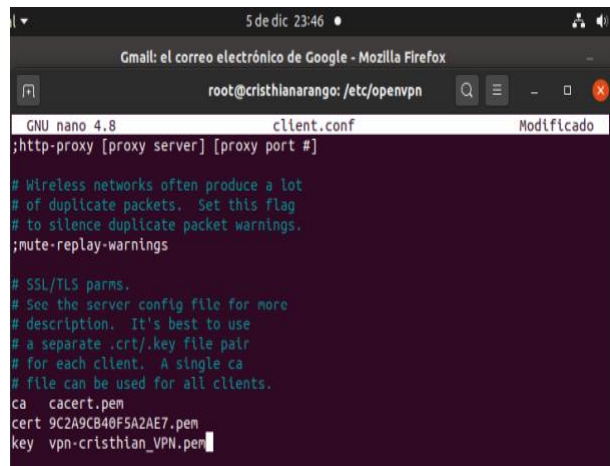


Figura 68. Configuración de conexión de OpenVPN.

Instalación de openvpn en la máquina de escritorio Ubuntu y más adelante se descomprime los archivos generados en Zentyal para el cliente en la ruta /etc/openvpn/.

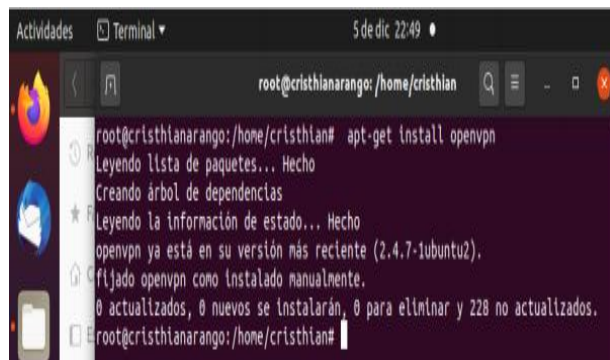


Figura 69. Instalación de OpenVPN.

Conexión con la VPN desde el escritorio Ubuntu.

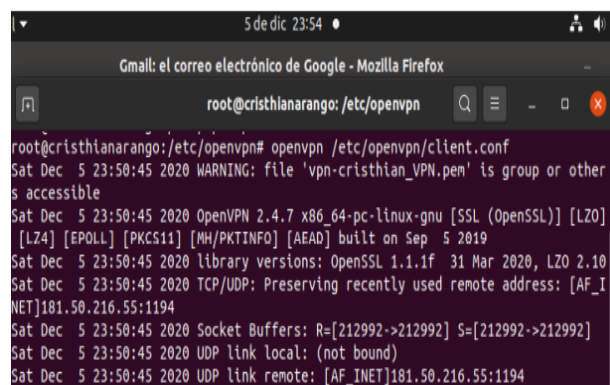


Figura 70. Conexión VPN desde escritorio Ubuntu.

Estatus de conexión a la VPN.

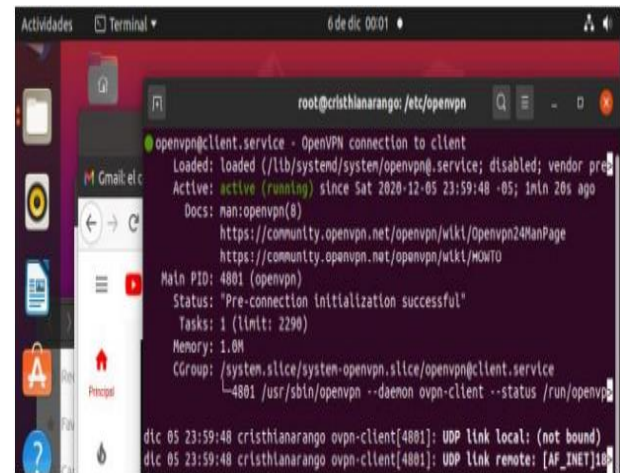


Figura 71. Estatus de conexión VPN.

II. Conclusiones.

Se realizó la instalación de Zentyal en la versión comercial más reciente (6.2) para dar manejo y administración de múltiples servicios que este nos ofrece.

Se estableció el control de acceso entre la estación GNU/Linux Ubuntu 18.04 mediante un controlador de dominio en Zentyal.

Se pudo configurar el modulo HTTP Proxy del servidor Zentyal, el cual brinda múltiples beneficios, entre los cuales, permite administrar los permisos de acceso a internet ya sea por perfiles, por dominios o por Ip's entre otros, a su vez este modulo permite acondicionar dichos permisos a horarios e inclusive por cargos que pueda tener una compañía.

Se logró dar gestión en Zentyal desde un navegador web para restringir el acceso a diferentes sitios de entretenimiento.

Se logró articular GNU/Linux Zentyal Server 6.2 para que pudiera acceder desde GNU Linux Desktop, previa implementación de servicios DHCP Server, DNS Server y controlador de dominios.

Se estableció un controlador de dominio único que permitió el acceso de una estación de trabajo GNU/Linux Desktop mediante usuario y contraseña previamente definidos en Zentyal.

REFERENCIAS

- [1] G. Obregón-Pulido, B. Castillo-Toledo and A. Loukianov, "A globally convergent estimator for n frequencies", IEEE Trans. On Aut. Control. Vol. 47. No 5. pp 857-863. May 2002.
- [2] H. Khalil, "Nonlinear Systems", 2nd. ed., Prentice Hall, NJ, pp. 50-56, 1996.

- [3] Manuales Zentyal. Recuperado el 10 de diciembre del 2020 de
[https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_\(VPN\)_con_OpenVPN](https://wiki.zentyal.org/wiki/Es/3.5/Servicio_de_redes_privadas_virtuales_(VPN)_con_OpenVPN)
- [4] Zentyal community, Gestion de máquinas virtuales. Documentación de Zentyal 6.2. (2018). Recuperado de.
<https://doc.zentyal.org/es/virt.html>

Notas:

1. Al realizar los cambios en el servidor Zentyal es indispensable pulsar la opción Guardar y esperar a que los cambios se apliquen satisfactoriamente.